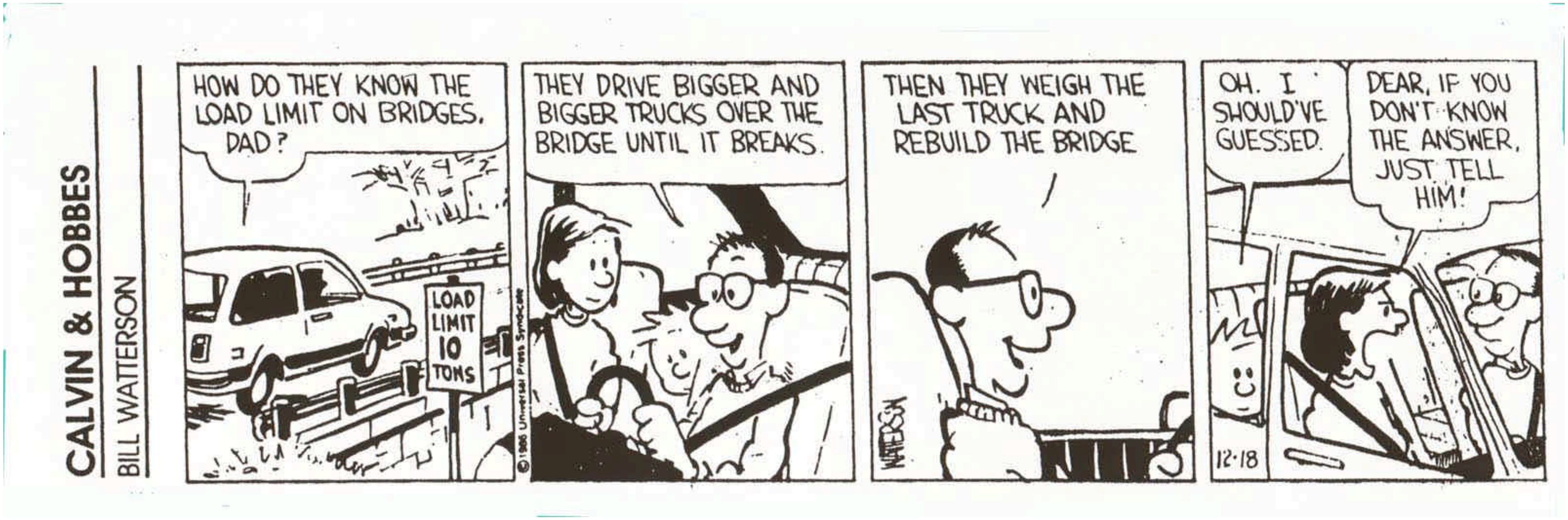
The Inherent Values of Probabilistic Risk Assessment

Second NASA Probabilistic Risk Assessment Workshop
June 19, 2001

Michael A. Greenfield, Ph.D.
Deputy Associate Administrator
Office of Safety and Mission Assurance
NASA Headquarters

Quantifying Risk in the Old Days w/o PRA


CALVIN & HOBBES
BILL WATTERSON
HOW DO THEY KNOW THE LOAD LIMIT ON BRIDGES, DAD?
LOAD LIMIT 10 TONS
© 1986 Universal Press Syndicate
THEY DRIVE BIGGER AND BIGGER TRUCKS OVER THE BRIDGE UNTIL IT BREAKS.
THEN THEY WEIGH THE LAST TRUCK AND REBUILD THE BRIDGE.
WATTERSON
OH. I SHOULD'VE GUESSED.
DEAR, IF YOU DON'T KNOW THE ANSWER, JUST TELL HIM!
12-18

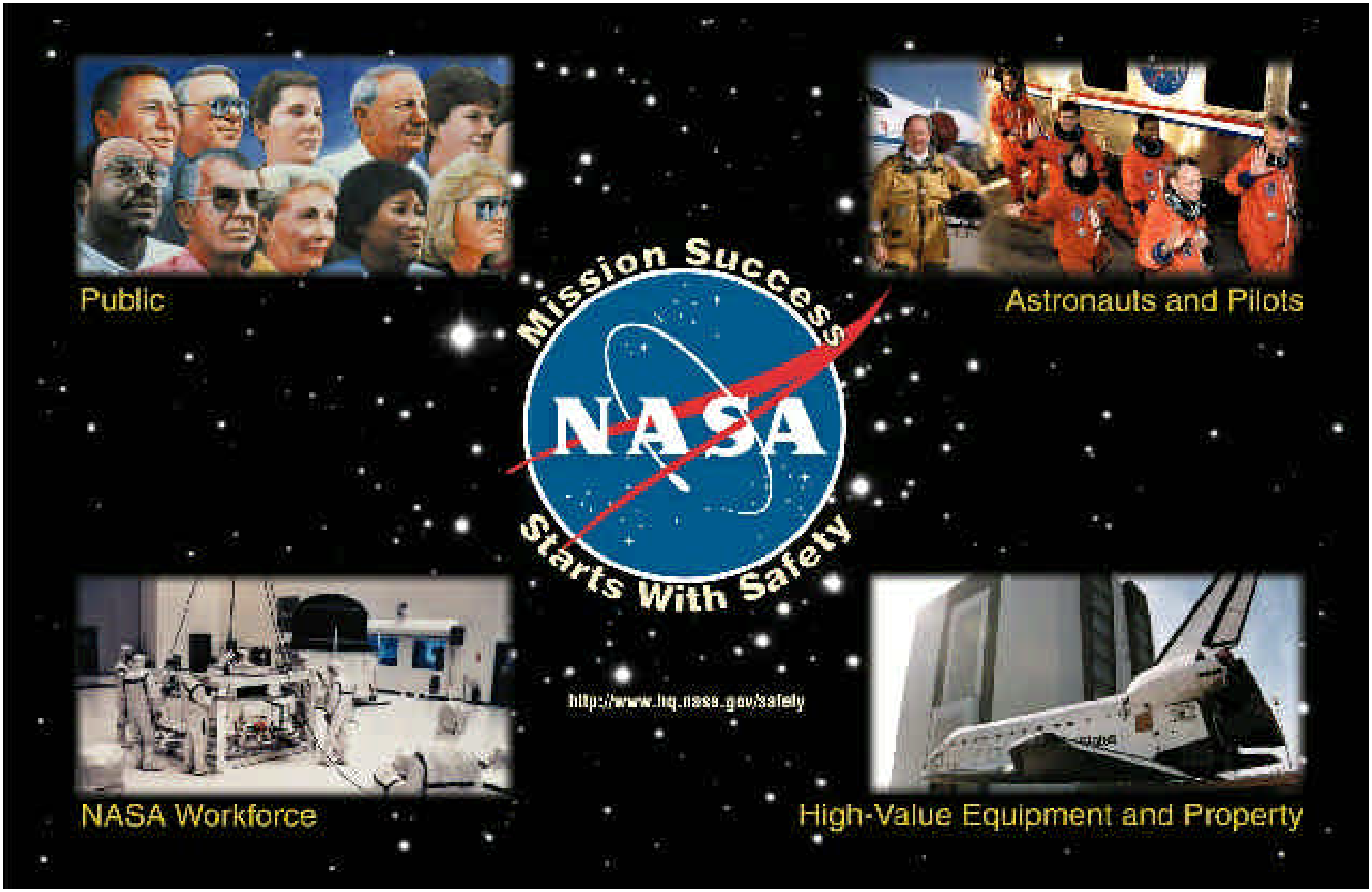
Quantifying Risk Today with PRA

The “Initiating Event” or why we’re here today:

> ***“Since I came to NASA [1992], we’ve spent billions of dollars on Shuttle upgrades without knowing how much they improve safety. I want a tool to help base upgrade decisions on risk.”***

Dan Goldin, NASA Administrator
July 29, 1996

More Reasons for PRA...


Public
Astronauts and Pilots
Mission Success Starts With Safety
NASA
http://www.hq.nasa.gov/safety
NASA Workforce
High-Value Equipment and Property

Draft PRA Policy Requirements

CONSEQUENCE CATEGORY	CRITERIA / SPECIFICS		NASA PROGRAM/PROJECT (Classes and/or Examples)	PRA SCOPE*
Human Safety & Health	Public Safety	Planetary Protection Program Requirement	Mars Sample Return	F
		White House Approval (PD/NSC-25)	Nuclear payload (e.g., Cassini, Ulysses, Galileo)	F
	Human Space Flight		International Space Station	F
			Space Shuttle	F
			Crew Return Vehicle	F
Mission Success (for non-human rated missions)	High Strategic Importance		Mars Program	F
	High Schedule Criticality		Launch window (e.g., planetary missions)	F
	Higher-Cost Missions (>$100M)		Earth Science Missions (e.g., EOS)	L
			Space Science Missions (e.g., SIM)	L
			Technology Demonstration and Validation (e.g., EO-1)	L
	Lower-Cost Missions (<$100M)		Earth Science Missions (e.g., QUICKSCAT)	L or N
			Space Science Missions (e.g., HESSI)	L or N
			Technology Demonstration and Validation (e.g., Deep Space 1)	L or N

(*) LEGEND: F = Full Scope; L = Limited Scope; N= None

NASA Scenario-Based PRA Methodology

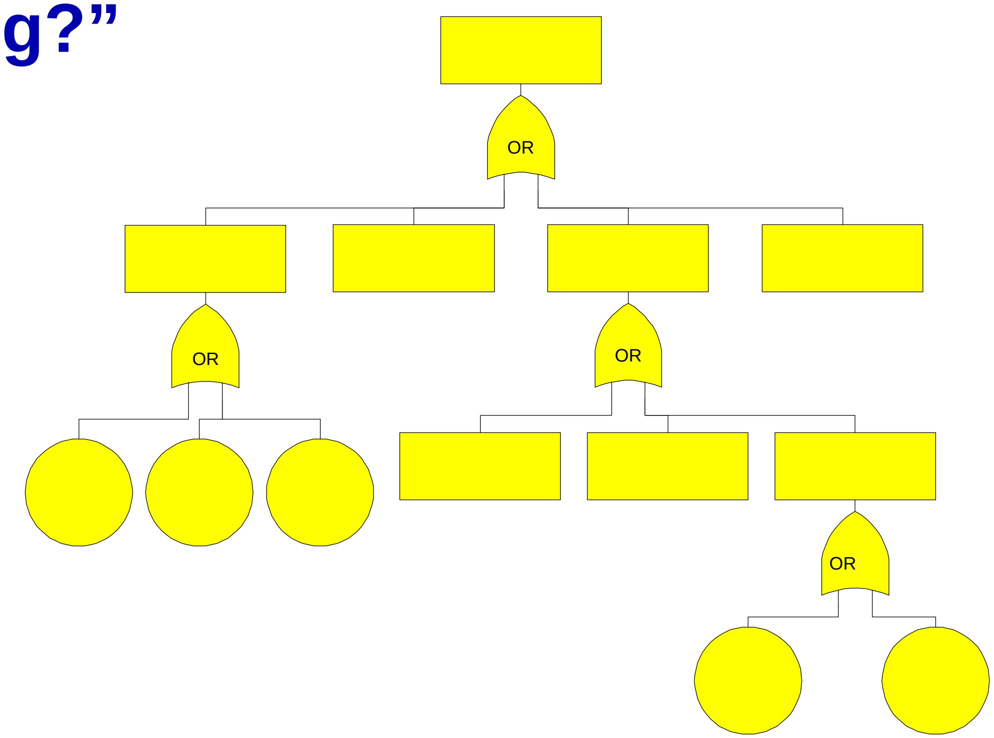
1. Identification of end-states of interest (related to PRA purpose)
2. System familiarization ("as-is" information) and data collection
3. Identification, selection, screening of initiation events, or IEs, (may require high-order logic model; e.g., master logic diagram (MLD))
4. Definition and modeling of all scenarios linking each IE, by way of pivotal events (PEs), to its logical end states, using event sequence diagrams (ESDs) or event trees (ETs)
5. Modeling of PEs using fault trees (FTs)
6. Risk quantification for each IE, PE, and scenario, and then aggregation of the risk for all like end states
7. Uncertainty analysis and sensitivity analysis as needed
8. Risk importance ranking for identification of risk drivers

The Inherent Values of PRA

- The individual elements of the PRA process have value in their own right
  - Master Logic Diagram (MLD)
  - Event Sequence Diagrams (ESD)
  - Fault Trees (FT)
  - Numerical results
- The integrated PRA has its own value that is greater even than the sum of the parts

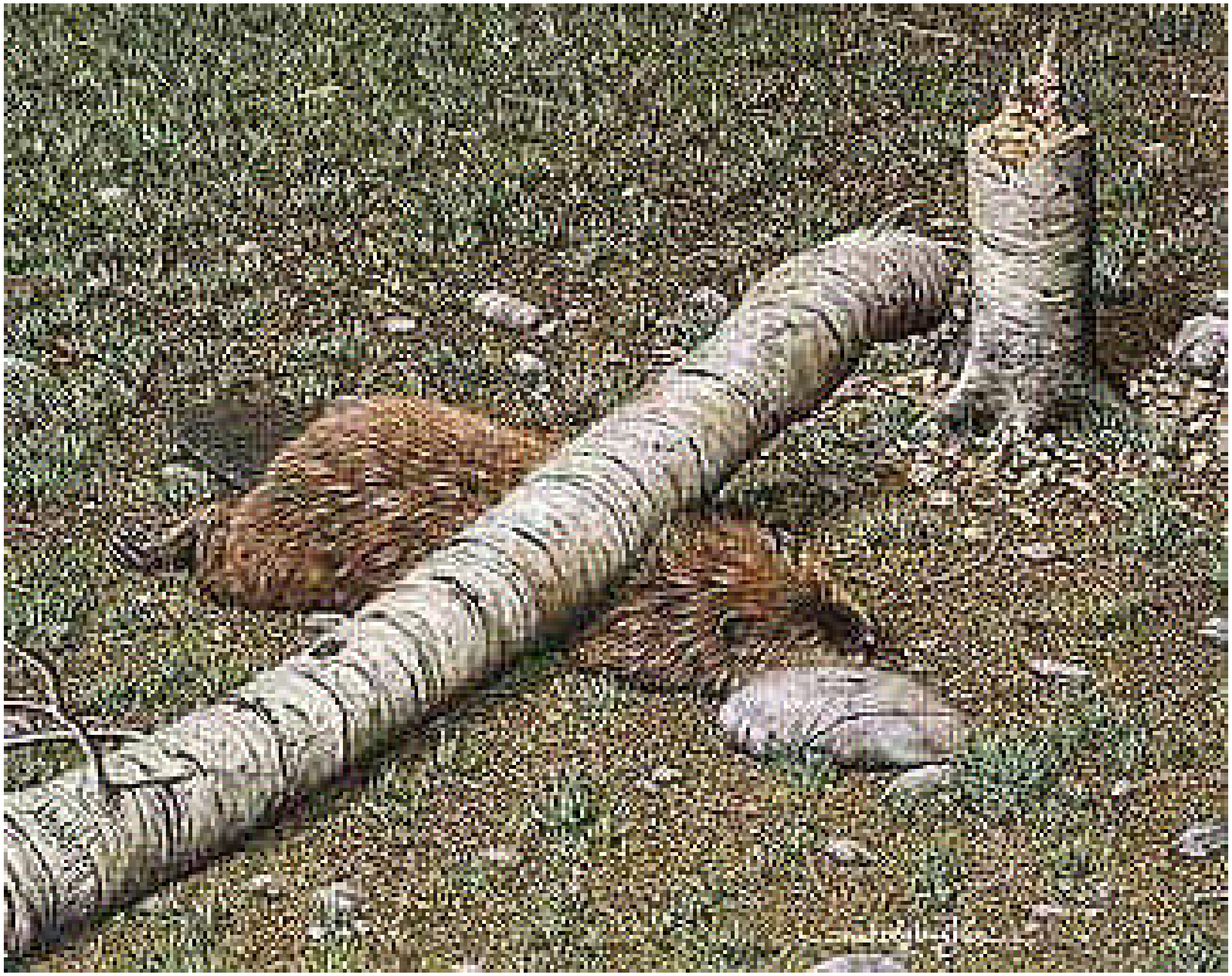
The Value of Master Logic Diagrams

- Help identify the initiating events that can lead to accidents or mission failure; i.e., “What could go wrong?”



Note: An MLD is essentially a high-level fault tree.

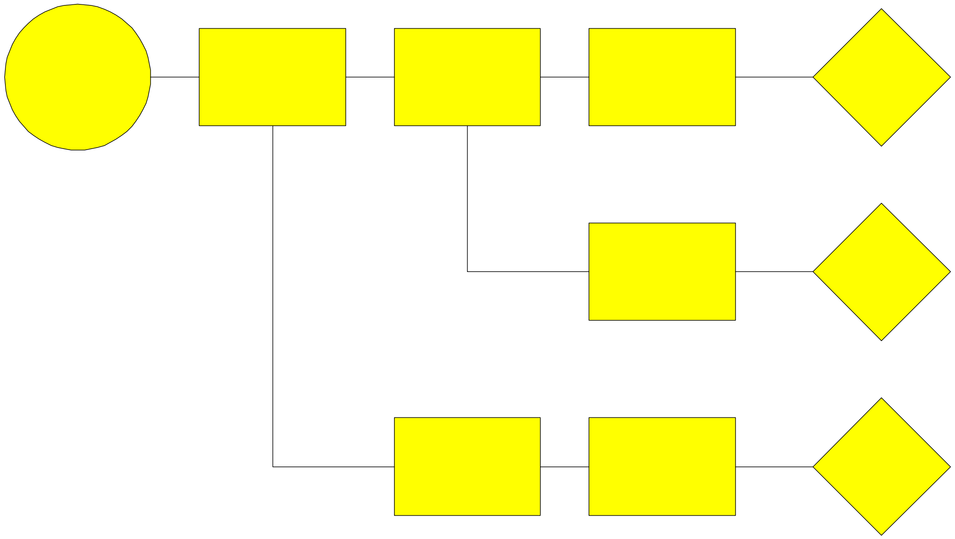
A simple high-level Fault Tree (MLD) might have anticipated this Tree Fault*



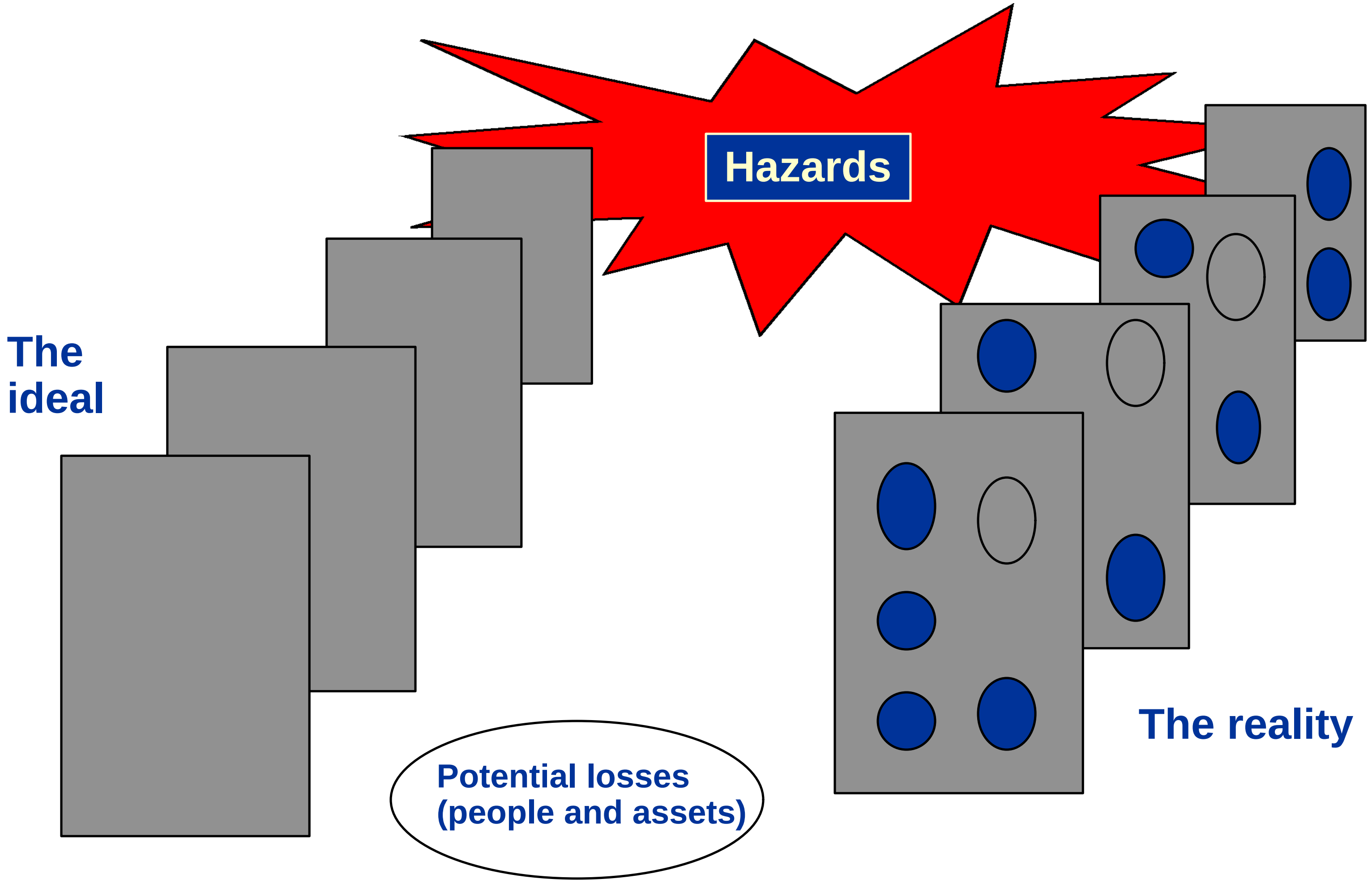
*Note: No beavers were harmed in making this chart.

The Value of Event Sequence Diagrams

- Identify accident scenarios
- Identify pivotal events or “defenses” to prevent the progression of accident scenarios to undesired end states

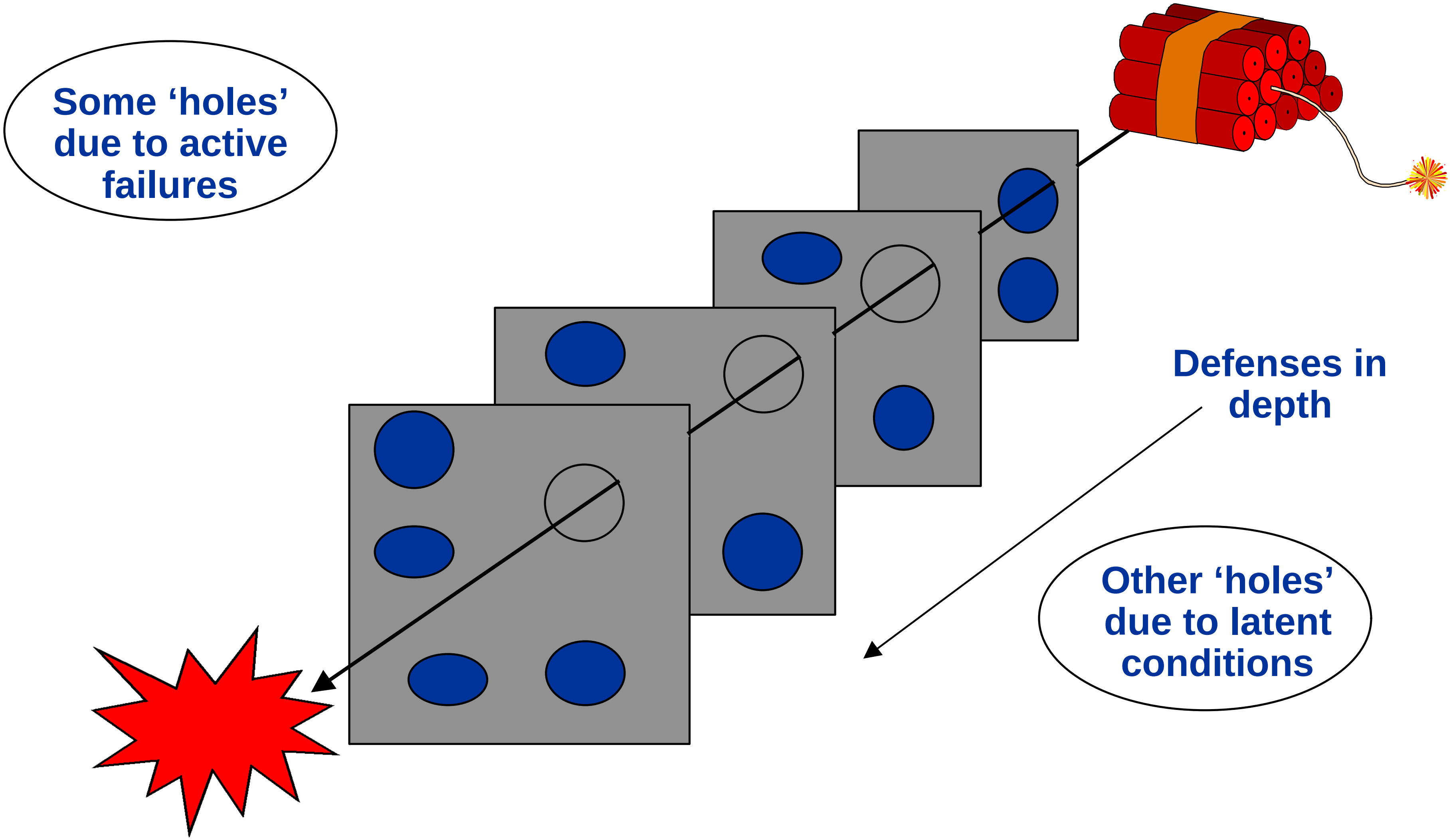


"Swiss Cheese" Model of Defenses



From "Managing the Risks of Organizational Accidents," James Reason

"Swiss Cheese" Model of Defenses



Some 'holes' due to active failures

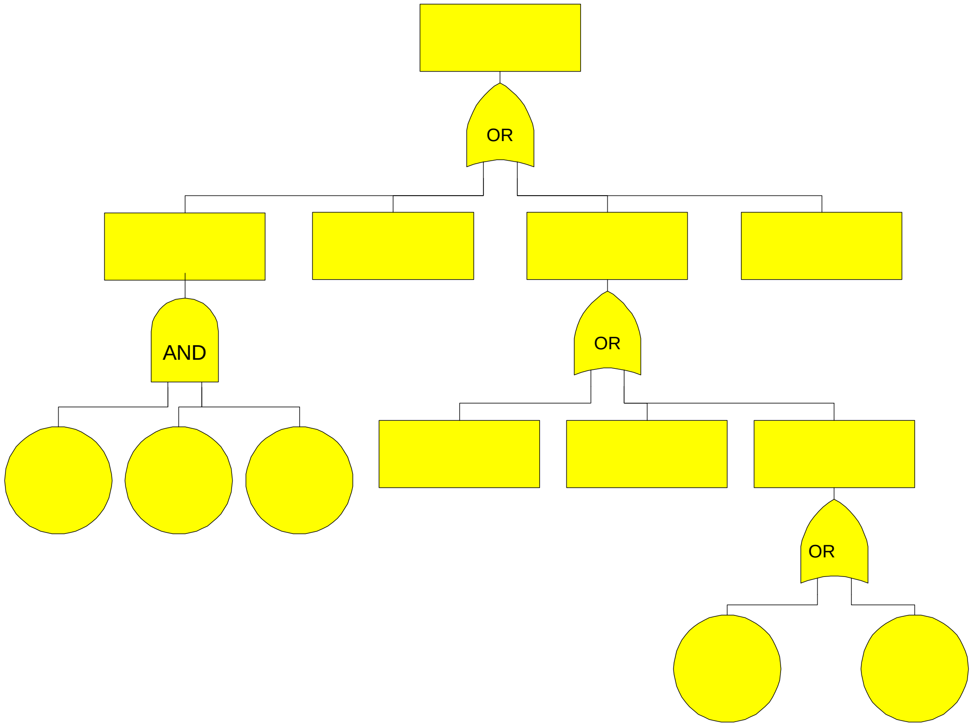
Defenses in depth

Other 'holes' due to latent conditions

From "Managing the Risks of Organizational Accidents," James Reason

The Value of Fault Trees

- Identify the basic events that could result in failure of “defenses”
  - Failed defenses are the “holes in the cheese”



The Value of the Numerical Results of PRA

- Enable one to respond to those who demand "Give me the numbers."
- Allow one to express the uncertainty in one's state of knowledge
  - Show where our knowledge is lacking so that it can be improved
- Provide a relative ranking of "risk drivers"
  - Show where to concentrate limited resources for maximum risk reduction
    - Especially valuable for FBC projects

The Value of an Integrated PRA

- Enables one to maintain configuration of the model up-to-date with configuration of the system
  - Challenge: How to make PRA models most easily maintainable?
- Has potential for use as a real-time risk monitor for individual unique missions
  - Challenge: How to realize this potential?
- Facilitates “what-if” analyses
  - Great way to analyze proposed design changes (including upgrades for operational programs)
- Provides basis for risk-based maintenance
- Provides basis for risk-based decision-making

“If eternal vigilance is the price of liberty, then chronic unease is the price of safety."

- James Reason, “Managing the Risk of Organizational Accidents”

And what better way than PRA to put your “chronic unease” to work?